

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with khepp1020@gmail.com and kbehling916@gmail.com (the “accounts”) that are stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (“Google”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 17, 2022 with the Google Reference Number 25457714, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from April 19, 2021 to present, unless otherwise indicated:

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the accounts, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;
- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;
- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;
- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App Activity, including:

search terms; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
- **WEB-BASED CHATS:** The contents of all chats associated with the accounts, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;
- **MOBILE MESSAGING:** The contents of all messages associated with the accounts, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery numbers; usernames and other identifiers; user settings; and all associated logs and change history;

Google is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 666, 1343, and 371 and, since April 19, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters, persons, or entities:

- a. Records and information relating to the City of Milwaukee's property;
- b. Records and information relating to a conspiracy to defraud the City of Milwaukee;
- c. Records and information relating to communications with other City of Milwaukee employees, to include Lonnie Fischer, Kyle Hepp, and Kelly Behling;
- d. Records and information relating to communications with Richard Gillis, Linda Simcakoski, and other purchasers or potential purchasers of City of Milwaukee property;
- e. Records and information relating to the sale or resale of vehicles and equipment;
- f. Records and information relating to the origins or whereabouts of vehicles and equipment offered for sale;
- g. Records and information relating to the finances—including but not limited to expenditures, obligations, income, and any financial or monetary transfers—of Kyle Hepp, Kelly Behling, Lonnie Fischer, Richard Gillis, and Linda Simcakoski;
- h. Records and information relating to the deletion of electronic evidence;
- i. Records and information related to possible criminal prosecutions, relevant criminal laws, and investigative methods;
- j. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);

- k. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- l. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- m. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation, including interests and motivations; and
- n. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Mar 16, 2023

s/ JDH

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information associated with khepp1020@gmail.com and
kbebling916@gmail.com (the "accounts") that are stored at premises owned,
maintained, controlled, or operated by Google LLC, a company
headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.Case No. **23-M-335 (SCD)**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the
person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 666; 18 U.S.C. § 1343; and 18 U.S.C. § 371.	State or local program fraud, theft or bribery concerning programs receiving federal funds; wire fraud; and conspiracy.

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Eric Burns

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone _____ (specify reliable electronic means).

Date: 03/16/2023

Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Eric Burns, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(I)(A) to require Google LLC (hereafter "Google") to disclose to the government records and other information, including the contents of communications, associated with the Google accounts associated with the email addresses khepp1020@gmail.com and kbehling916@gmail.com, that are stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I have been a Special Agent with the FBI since November 2009. I am currently assigned to an FBI squad which investigates financial crimes, civil rights crimes, and public corruption crimes. During my tenure with the FBI, I have participated in investigations involving the corruption of public officials, to include facilitation payments and kickbacks. I have participated in all aspects of investigations including executing search warrants involving, among other things, the search and seizure of computers, computer equipment, software, and electronically stored information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 18 U.S.C. §§ 666, 1343, and 371, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(I)(A), & (c)(I)(A). Specifically, the Court is “a district court of the United States ... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

The Overall Scheme

6. The FBI is investigating allegations of fraud and abuse by several City of Milwaukee (“City”), Department of Public Works (“DPW”) employees who conspired to sell City-owned equipment and vehicles to friends and amongst each other at prices significantly below market value, rather than using the City-approved auction house. As further detailed below, these friends in turn posted and sold the City-owned equipment and vehicles on Facebook Marketplace at substantially higher prices than what they purchased them for from the City.

7. On or about August 17, 2020, LONNIE FISCHER was hired as DPW’s Fleet Services Manager. On or about April 19, 2021, KYLE HEPP was hired as DPW’s Fleet Acquisitions Manager. KELLY BEHLING has worked for the City since April 2014 in various administrative support roles, but most recently served as a DPW Program Assistant in Fleet Services since on or about April 4, 2021. Together, FISCHER, HEPP, and BEHLING were responsible for, amongst other things, overseeing DPW’s equipment disposal process, decommissioning DPW equipment, and preparing/selling surplus DPW equipment.

8. According to an anonymous complaint filed with DPW's Fraud Hotline on September 20, 2022, since being hired as DPW's Fleet Services Manager, FISCHER has been hiring his friends to staff the Fleet Services department, to include hiring HEPP as the Fleet Acquisitions Manager. The anonymous complainant stated HEPP was taking City-owned equipment, ranging from small tools to vehicles, and selling it to his friends, RICK GILLIS and LINDA SIMCAKOSKI, rather than taking the City-owned equipment to auction. According to the anonymous complainant, GILLIS and SIMCAKOSKI then posted and sold the City-owned equipment on Facebook Marketplace at a profit.

9. The anonymous complaint prompted a review of DPW's files, which corroborated many of the details in the complaint. According to information provided by DPW's interim Fleet Services Manager ("INDIVIDUAL-1"), who has been conducting an extensive review of DPW's used equipment sales between January 1, 2020 and September 29, 2022, the City has been defrauded of at least \$480,000, due, at least in part, to City-owned equipment and vehicles being sold to individuals at prices significantly below market value rather than using the City-approved auction house to conduct arms-length transactions. INDIVIDUAL-1 has also identified several instances of non-City vehicles being used to remove loads of equipment and surplus items from City facilities. City records revealed GILLIS to be the largest benefactor of City-owned equipment and vehicles being sold to individuals at prices significantly below market value.

10. According to information provided by INDIVIDUAL-1, between June 17, 2022 and September 8, 2022, GILLIS purchased at least 74 items of City-owned equipment or vehicles for approximately \$35,130. INDIVIDUAL-1 assessed a fair market value of these items at approximately \$315,850, based on what the City could have received using the City-approved auction house.

Accounts and Contacts

11. According to information received by subpoena from Meta, Facebook account 100002043280466 is registered to email address gillisteam@hotmail.com and subscribed to a “Rick Gillis” (the “Gillis Facebook Account”). The Gillis Facebook Account was created or about January 1, 2011.

12. According to information received by subpoena from Meta on November 7, 2022, Facebook account 1304449376 is registered to email address slippery12no@yahoo.com and is subscribed to a “Linda Simcakoski” (the “Simcakoski Facebook Account”). The Simcakoski Facebook Account was created on or about February 12, 2012.

13. According to information received by subpoena from U.S. Cellular, telephone number 262-312-0107 has been subscribed to by HEPP since November 2, 2015. HEPP is listed as the financially liable party with a billing address of 111 Richard Street, Waukesha, WI 53189.

14. According to information received by subpoena from T-Mobile, telephone number 414-210-8076 has been subscribed to by BEHLING since May 29, 2017. BEHLING is listed as the financially liable party with a billing address of 2045 S. 34th St., Milwaukee, WI 53215.

15. According to information received by subpoena from Google, Google account 360528787251 is registered to email address khepp1020@gmail.com (“Account-1”) and is subscribed to a “K Rhe” with recovery telephone number 262-312-0107, the telephone number subscribed to by HEPP. Account-1 was created on October 15, 2009, and Account-1 was logged into as recently as November 2022. According to information provided by Google, Account-1 uses the following Google services: Gmail, Google Services, Google Hangouts, Google Drive, Google Calendar, Google Docs, Android, YouTube, Google Chrome Sync, Location History, Google

Photos, Google Cloud Print, Google Play, Google My Maps, Google Keep, Google Payments, Chromeos Login.

16. A review of Account-1's IP activity, received via subpoena, revealed Account-1 has been accessed over 1,100 times since February 2022. Between June 17, 2022 and September 8, 2022, which corresponds to the period in which GILLIS purchased City-owned equipment or vehicles, Account-1 was accessed at least 190 times. Since September 20, 2022, the date the anonymous complaint was filed with DPW's Fraud Hotline, Account-1 has been accessed at least 700 times.

17. According to information received by subpoena from Google, Google account 80064961146 is registered to email address kbehling916@gmail.com ("Account-2") and is subscribed to a "Kelly Behling" with recovery telephone number 414-210-8076, the telephone number subscribed to by BEHLING. Account-2 was created on August 30, 2011, and Account-2 was also logged into as recently as November 2022. According to information provided by Google, Account-2 uses the following Google services: Web & App Activity, Gmail, Google Hangouts, iGoogle, Android, Google Calendar, YouTube, Google Voice, Google Drive, Google Chrome Sync, Google Photos, Location History, Google Play, Google Services, Google Cloud Print, Google Payments, Google My Maps, Play Loyalty, G1 Phone Backup, Dynamite.

18. A review of Account-2's IP activity, received via subpoena, revealed Account-2 has also been frequently accessed since February 2022. Between June 17, 2022 and September 8, 2022, which corresponds to the period in which GILLIS purchased City-owned equipment or vehicles, Account-2 was accessed at least 73 times. Since September 20, 2022, the date the anonymous complaint was filed with DPW's Fraud Hotline, Account-2 has been accessed at least 80 times.

19. Between November 12, 2021 and November 9, 2022, according to information received by subpoena, the telephone number subscribed to by HEPP exchanged over 6,000 text messages and over 400 telephone calls with the telephone number subscribed to by BEHLING, including on days and at specific times relevant to the SUBJECT OFFENSES, as further described below.

20. Between June 14, 2022 and November 8, 2022, according to information received by subpoena, the telephone number subscribed to by HEPP exchanged over a thousand calls and text messages with a telephone number subscribed to by GILLIS's wife and used by GILLIS, including on days and at specific times relevant to the SUBJECT OFFENSES, as further described below.

21. Between June 18, 2022 and September 28, 2022, according to information received by subpoena, the telephone number subscribed to by BEHLING exchanged 20 text messages and 10 telephone calls with a telephone number subscribed to by GILLIS's wife and used by GILLIS. Further, between June 21, 2021 and October 31, 2022, the telephone number subscribed to by BEHLING exchanged 4 text messages and 19 telephone calls with a telephone number subscribed to by FISCHER.

Specific Executions of the Scheme

22. A review of the Gillis Facebook Account, received via search warrant, revealed multiple postings for equipment and vehicles for sale that had been "purchased" for far less from the City of Milwaukee. For example, on July 27, 2022, the Gillis Facebook Account listed a 2010 Wain Roy concrete breaker that came off a John Deere 410J for sale at \$3,999.

23. On July 26, 2022, according to DPW records, the City recorded the sale of a John Deere 410J for \$2,000 to GILLIS¹.

24. On July 26, 2022, according to information received by subpoena, the telephone number subscribed to by HEPP exchanged 32 text messages and one telephone call with the telephone number subscribed to by BEHLING. Additionally, on July 26, 2022, the telephone number subscribed to by HEPP exchanged seven text messages and two telephone calls with the telephone number used by GILLIS.

25. A review of the Simcakoski Facebook Account, received via search warrant, also revealed multiple postings for equipment and vehicles for sale. For example, in August 2022, the Simcakoski Facebook Account listed a 2004 John Deere 410G Backhoe Loader for sale at \$27,999.

26. On August 14, 2022, according to DPW records, the City recorded the sale of a 2004 John Deere 410G for \$2,000 to GILLIS¹. INDIVIDUAL-1 estimated the backhoe's value to be \$35,000.

27. On September 28, 2022, according to information received by subpoena from Landmark Credit Union, GILLIS deposited a check into his savings account for \$26,500. The memo line on the check stated, "John Deere 410G."

28. With respect to the instances of non-City vehicles being used to remove loads of equipment and surplus items from City facilities, as indicated above, these instances appear to have been coordinated by several DPW employees, to include HEPP and BEHLING, without authorization from the City. For example, surveillance footage of DPW's Central Repair Garage revealed that on Saturday, August 20, 2022, 22 pallets of various materials, six pieces of welding

¹ Please note that in other legal process in this matter, your Affiant incorrectly described this specific transaction as the date GILLIS purchased the item from the City. This is more accurately described as the date the City recorded the sale of the item, which may or may not have corresponded with the date GILLIS took possession of the item.

equipment, and a new replacement fuel tank for a City-owned truck, were removed from the secure stockroom and loaded onto a large platform truck and a stake bed truck. DPW's surveillance footage shows HEPP and BEHLING assisting in the removal of these items, and GILLIS present at the scene. INDIVIDUAL-1 assessed a fair market value of these items at approximately \$53,186, based on what the City could have received using the City-approved auction house or, to the extent the items could not be auctioned, recycling the items.

29. According to information provided by INDIVIDUAL-1, DPW has one bill of sale on file to reflect the August 20, 2022 "sale" of the 22 pallets, six pieces of welding equipment, and the new replacement fuel tank for a City-owned truck. The bill of sale indicates three obsolete welders were sold to GILLIS on August 20, 2022 for \$150.00.

30. Between August 19, 2022 and August 20, 2022, according to information received by subpoena, the telephone number subscribed to by HEPP exchanged 67 text messages and 11 telephone calls with the telephone number subscribed to by BEHLING. Additionally, between August 19, 2022 and August 20, 2022, the telephone number subscribed to by HEPP exchanged 11 text messages and 11 telephone calls with the telephone number used by GILLIS.

31. On January 5, 2023, the aforementioned City-owned replacement fuel tank that was removed from DPW's Central Repair Garage on August 20, 2022 was identified as being listed for sale on GILLIS' Facebook Marketplace page. The fuel tank, which cost the City \$1,000, was listed for sale for \$650.00.

32. On January 7, 2023, an FBI Undercover Employee (UCE-1) sent a message to GILLIS via Facebook Messenger expressing an interest in purchasing the City-owned replacement fuel tank. GILLIS responded that the fuel tank was still available and asked for UCE-1's telephone number.

33. On January 10, 2023, at approximately 5:11pm CST, UCE-1 attempted to place a consensually recorded telephone call to GILLIS (on the phone number subscribed to his wife, which GILLIS uses), which was verified using the FBI's telephonic consensual monitoring system. GILLIS did not answer and UCE-1 did not leave a voicemail.

34. On January 10, 2023, at approximately 5:22pm CST, which is approximately 11 minutes after UCE-1 attempted to place a consensually recorded telephone call to GILLIS, according to information received by court order, the telephone number subscribed to by HEPP received one text message from the telephone number used by GILLIS. Less than a minute later, the telephone number subscribed to by HEPP sent one text message to the telephone number used by GILLIS.

35. On January 10, 2023, at approximately 7:11pm CST, UCE-1 placed a consensually recorded telephone call to GILLIS (on the phone number subscribed to his wife, which GILLIS uses), which was verified using the FBI's telephonic consensual monitoring system. GILLIS informed UCE-1 that the fuel tank listed for sale was brand new, that it was \$650.00, and that GILLIS wanted cash as payment for the fuel tank. UCE-1 and GILLIS agreed to touch base on January 12, 2023 to arrange for a time on January 12, 2023 for UCE-1 to inspect and purchase the fuel tank.

36. On January 12, 2023, UCE-1 and another FBI Undercover Employee (UCE-2) met GILLIS at GILLIS' residence. UCE-1 and UCE-2 were both equipped with audio and video recording software, which I have since listened to and watched. As UCE-1 and UCE-2 drove their vehicle up the driveway of GILLIS' residence, they pointed out several items located on GILLIS' property, to include a Freightliner truck, a trencher, a large trailer bearing the numbers "56733," and a flatbed truck. UCE-1 and UCE-2 proceeded to the front door of GILLIS' residence, where

they were greeted by GILLIS. GILLIS walked UCE-1 and UCE-2 to a pole barn located on his property. Located inside the pole barn was the fuel tank UCE-1 and UCE-2 intended to purchase, along with numerous boxes that appeared to be filled with used tools and equipment. The pole barn also contained a large compressor, which UCE-1 inquired about. GILLIS stated it was his father-in-law's, but that he had not run power to it yet because he "[didn't] like getting [his] hands dirty, I buy and sell shit, that's it." GILLIS also told UCE-1 and UCE-2 that the pole barn where the fuel tank was located "was nothing," and that he had "a warehouse twice this size and it's full of just shit," but that he had "no time to list shit." UCE-2 asked GILLIS if he had anything for their purported landscaping business. GILLIS stated, "I did have lots of stuff, I had grapple buckets, I had grader buckets, I had equipment, I had backhoes, I had tractor backhoes, I was buying all kinds of shit this summer and then everything just kind of went pleh." In discussing used equipment purchasing, GILLIS also said, "municipal equipment's pretty good." He also stated that he had purchased two "Bobcats," used them all summer, and then sold them without losing any money.

37. At the end of the meeting, UCE-2 asked GILLIS if the fuel tank was \$650.00 and GILLIS responded, "give me \$600.00." UCE-2 handed GILLIS \$600.00 in U.S. Currency and UCE-1 and UCE-2 loaded the box containing the fuel tank into their vehicle. GILLIS returned to his residence with the \$600.00 in U.S. Currency received from UCE-2.

38. On January 12, 2023, after UCE-1 and UCE-2 transported the box containing the fuel tank to an FBI evidence warehouse, I inspected the box. I observed a torn label on the box, which stated, in part, "STOCKROOM COPY." In reviewing the surveillance footage from the aforementioned August 20, 2022 incident at DPW's Central Repair Garage wherein a new replacement fuel tank for a City-owned truck was removed from the secure stockroom and loaded onto a large platform truck and a stake bed truck, and where GILLIS was present when this

occurred, I observed a torn label on the box containing the fuel tank that appears to be identical to the torn label on the box containing the fuel tank UCE-1 and UCE-2 purchased from GILLIS on January 12, 2023.

39. On August 22, 2022, according to DPW records, the City recorded the sale of a 1990 Landa Steam Cleaner 1200 PSI Trailer to GILLIS for \$136.36. The City's equipment identification number for that item is 56733, which is the same number the large trailer exhibited that was located on GILLIS' property when UCE-1 and UCE-2 met GILLIS on January 12, 2023, as indicated above. INDIVIDUAL-1 assessed a fair market value of approximately \$1,000 for that item.

Personnel Actions and Prior Investigation

40. According to information provided by DPW, FISCHER, HEPP, and BEHLING were all placed on administrative leave immediately after DPW received the anonymous complaint. FISCHER, HEPP, and BEHLING have all since resigned from DPW in lieu of discharge.

41. On December 21, 2022, HEPP consented to a pre-discharge hearing interview conducted by the City, at which time HEPP was presented with a *Garrity* Warning and *Garrity* Waiver documents. HEPP signed the *Garrity* Waiver. During the interview, HEPP stated that he determined the price of the equipment and vehicles the City sold, to include the equipment and vehicles the City sold to GILLIS, whom he met in 2021. HEPP stated he just looked at the overall condition of the equipment or vehicle and set the price. HEPP stated he understood that he should not have made sales in the manner he did, but blamed FISCHER, stating FISCHER directed this manner of disposal because FISCHER was irritated that DPW had to answer so many questions when selling equipment or vehicles via auction. HEPP denied profiting from the manner in which

purchases and sales of City-owned equipment and vehicles were conducted, but indicated he received a benefit because he was able to “use” a vehicle someone he knew purchased from the City. HEPP was also confronted with a picture of a truck he purchased from the City at substantially less than its market value, and subsequently admitted that it was improper to set the value and also purchase the vehicle. With respect to the August 20, 2022 incident at DPW’s Central Repair Garage, HEPP admitted he was present and acknowledged non-City individuals, to include GILLIS, were on site. HEPP claimed that FISCHER told him to get rid of stuff, and was therefore doing what he was doing at the direction of FISCHER.

42. On December 29, 2022, BEHLING consented to a pre-discharge hearing interview conducted by the City, at which time BEHLING was presented with a *Garrity* Warning and *Garrity* Waiver documents. BEHLING signed the *Garrity* Waiver. During the interview, BEHLING reiterated much of what HEPP said during his pre-discharge hearing interview, but with some minor deviations. According to BEHLING, FISCHER directed the manner of disposal of equipment and vehicles because the process to auction was too cumbersome; however, FISCHER was responsible for deciding which vehicles would be sold to whom and what value they would be assigned. BEHLING stated she also knew GILLIS and that GILLIS bought and subsequently sold the equipment and vehicles he acquired from the City. Like HEPP, BEHLING denied profiting from the manner in which purchases and sales of City-owned equipment and vehicles were conducted, but did admit to purchasing a vehicle from the City for her daughter for \$400.00 (INDIVIDUAL-1 estimated the fair market value of the vehicle to be \$4,400).

43. On January 4, 2023, prior to a pre-discharge hearing scheduled for FISCHER, FISCHER emailed a Human Resources Representative at DPW requesting DPW allow him to resign from DPW in order to seek other employment prior to the hearing. In that email, FISCHER

stated, “I am taking full accountability for all items listed in your email.” FISCHER ultimately resigned from DPW prior to the hearing and therefore did not consent to an interview.

44. According to information received via subpoena from Potawatomi Casino, HEPP and BEHLING both frequent the casino. The sums of money they were each gambling increased dramatically during the summer of 2022, when the above-described scheme was at its most active.

Prior Search Warrants

45. On February 13, 2023, law enforcement executed a search warrant of GILLIS’ residence pursuant to a lawful court order dated February 10, 2023. *See* 23-MJ-17. While executing the search warrant, law enforcement also interviewed GILLIS. GILLIS stated, in part, that he was introduced to HEPP by HEPP’s brother, who GILLIS worked with. GILLIS stated HEPP’s brother turned GILLIS on to purchasing items from DPW. GILLIS further stated that he always purchased items from HEPP and that HEPP told GILLIS that GILLIS had to pay for items in cash. GILLIS also stated that law enforcement was mistaken about what he had paid for vehicles and equipment he purchased from DPW. For example, GILLIS claimed he purchased the 2004 John Deere 410G, as previously discussed in this Affidavit, for \$13,000 from the City, not \$2,000. GILLIS retrieved receipts he received from the City when he purchased vehicles and equipment, which law enforcement subsequently seized as part of the aforementioned search warrant. GILLIS identified the receipt in question, which law enforcement observed to be nearly identical to the receipt maintained by DPW (but with a different sales price), which indicated GILLIS paid \$13,000 for the item. When asked why the receipt maintained by DPW would indicate GILLIS paid a different value for an item than the one GILLIS had in in possession, GILLIS stated he did not know but that he always signed two receipts when he met HEPP at DPW to purchase an item. GILLIS also told law enforcement that after HEPP was placed on Paid Administrative Leave by DPW, HEPP

asked GILLIS, on at least two occasions, to get rid of his receipts. GILLIS indicated he was concerned by HEPP's request, and took steps to hide the receipts from HEPP for fear of HEPP destroying them.

46. On February 18, 2023, law enforcement executed a search warrant of HEPP's cellular telephone pursuant to a lawful court order dated February 9, 2023. *See* 23-MJ-19. While executing the search warrant, law enforcement also interviewed HEPP. During the interview, HEPP was shown the differing receipts for the 2004 John Deere 410G, that GILLIS purchased from the City, one receipt indicating it was sold to GILLIS for \$2,000 and the other indicating it was sold to GILLIS for \$13,000. When questioned about the differing amounts, HEPP stated, in part, that "there was no scheme. There was the thought of making profit, more money, that type of scenario, that's all it was." When asked who HEPP was referring to regarding who made "more money," HEPP stated, "I don't want to incriminate myself whatsoever."

47. A review of the contents of HEPP's cellular device revealed the following:

- a. Account-1 was used as the email service for the device. However, the device contained no emails to or from Account-1 before January 19, 2023, despite the frequent IP activity associated with Account-1 as indicated above.
- b. The device contained no internet search history prior to January 2, 2023.
- c. The device used the Chrome browser to access various accounts, to include Account-1.
- d. The earliest text message between HEPP and BEHLING is dated November 23, 2022, despite telephone records showing thousands of text messages between HEPP and BEHLING since November 2021.

- e. A review of the text messages between HEPP and BEHLING that were still contained on the device revealed HEPP and BEHLING, at times, discussed this investigation. For example, on December 19, 2022, HEPP and BEHLING exchanged screenshots of the letters they separately received from the City regarding their upcoming pre-discharge hearings. Notably, and in response to HEPP receiving a screenshot of BEHLING's pre-discharge hearing letter wherein the City alleged, in part, that BEHLING had "induced, or has attempted to induce, an officer or employee in the service of the city to commit an unlawful act or to act in violation of any lawful and reasonable departmental or official regulation or order...", HEPP sent BEHLING a screenshot of the definition of embezzlement.
- f. A further review of the text messages between HEPP and BEHLING revealed they likely coordinated their responses to the City in order to blame FISCHER. For example, on December 29, 2022, the day of BEHLING's pre-discharge hearing interview with DPW, HEPP stated "Thinking of you and remember, we did nothing wrong, they will try to say anything they can to pass the blame. We did what we were told by Lonnie." BEHLING responded, "Ik I'm just ready for it to be over. And I still don't see how the hell we get in trouble because of decisions Lonnie made..."
- g. Similar to BEHLING, the earliest text message between HEPP and GILLIS is dated November 21, 2022, despite telephone records showing text messages between HEPP and BEHLING since June 2022.

48. On February 22, 2023, law enforcement executed a search warrant of BEHLING's cellular telephone pursuant to a lawful court order dated February 22, 2023. *See* 23-MJ-49. A review of the contents of BEHLING's cellular device revealed the following:

- a. Account-2 was used as the email service for the device. However, the device contained no emails to or from Account-2 before November 23, 2022, despite the frequent IP activity associated with Account-2 as indicated above.
- b. The device primarily used the Chrome browser to access various accounts, to include Account-2.
- c. Similar to HEPP's cellular device, the earliest text message between BEHLING and HEPP is dated November 17, 2022, despite telephone records showing thousands of text messages between HEPP and BEHLING since November 2021.
- d. The earliest text message between BEHLING and FISCHER is dated December 7, 2022, despite telephone records showing 4 text messages between BEHLING and the telephone number subscribed to by FISCHER between June 21, 2021 and October 31, 2022, as previously stated.
- e. The device contained no text messages between BEHLING and GILLIS, despite telephone records showing 20 text messages with a telephone number used by GILLIS.

Evidence Likely Possessed by Google

49. Google is one of the world's most popular search engines. Google maintains google.com, a website which is accessible to most of the world. The records and information associated with Google accounts and IP addresses that used Google's search engines (including google.com) to conduct Google searches may assist law enforcement officers in determining when

and why HEPP and BEHLING deleted information from their cellular devices, as well as how the scheme to defraud the City was orchestrated.

50. Based on my training and experience, it is common for individuals who engage in criminal activities, such as fraud, to conduct Internet searches – in particular, Google searches – in support of their operations. Here, HEPP and BEHLING are alleged to have embezzled tens of thousands of dollars from the City and appear to have taken coordinated steps to delete information on their cellular devices relevant to the time period of the fraud. The results of the requested search warrant may provide information indicating Account-1 and/or Account-2 searched for ways to evade detection and mechanisms in which to delete information from an electronic device. The results of the requested search warrant may also include information that HEPP and BEHLING deleted from their phones, but that was preserved through their Google accounts.

51. Based on my training and experience, individuals who engage in criminal activities use methods to obfuscate their activity, such as deleting information from electronic devices. Indeed, neither HEPP nor BEHLING have text messages with each other on their cellular devices before November 17, 2022, despite telephone records showing thousands of text messages between them since November 2021. Further, and as previously stated, HEPP's cellular device's internet search history appears to have been deleted. The account activity, logs, stored electronic communications, and other data retained by Google for Account-1 and Account-2 can indicate who has used or controlled Account-1 and Account-2.

52. Based on my training and experience, I know that criminals utilize internet browsers, like Chrome, to conduct research and to find out what information is publicly available. Here, HEPP and BEHLING were placed on Paid Administrative Leave in September 2022 pending the outcome of this investigation. Because they were aware of this investigation by virtue of being

placed on Paid Administrative Leave pending its outcome, it is likely HEPP and BEHLING conducted research to find out what information was publicly available regarding the investigation and to determine how to avoid prosecution. For example, on December 19, 2022, HEPP sent BEHLING a screenshot of the definition of embezzlement, as discussed above. In this example, if HEPP utilized Chrome to search for the definition of embezzlement, Google maintains information associated with Account-1's cookies, which are messages that web servers pass to your web browser when you visit internet sites.

53. Based on my training and experience, I know that criminals may delete information saved to their digital devices, such as cellular telephones, to hide their criminal activities. However, that information may be saved by their service provider. For example, I know that Google can store a record of a customer's browser or map search history if the user is logged into their Google account. While a customer may clear their local search history, that information may still be stored on Google servers.

54. On October 17, 2022, a preservation request under 18 U.S.C. § 2703(f) was sent to Google regarding Google accounts registered under khepp1020@gmail.com and kbebling916@gmail.com, requesting Google preserve available data.

BACKGROUND CONCERNING GOOGLE²

55. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser

² The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lens.google.com; product pages on support.google.com; and product pages on about.google.com.

called Google Chrome, a free search engine called Google Search, and other services. Many of these free services offer additional functionality if the user signs into their Google Account.

56. In addition, Google offers an operating system for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

57. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

58. **GMAIL:** Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

59. **CONTACTS:** Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device

address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

60. **CALENDAR:** Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

61. **WEB-BASED CHATS and MOBILE MESSAGING:** Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention.

62. **GOOGLE DRIVE and GOOGLE KEEP:** Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage

limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called “Shared with me.” Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

63. **GOOGLE PHOTOS:** Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

64. **GOOGLE MAPS:** Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their

account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

65. **GOOGLE PAY:** A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile but Google Payment Corporation retains some records for regulatory purposes.

66. **GOOGLE CHROME and MY ACTIVITY:** Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account.

67. **GOOGLE PLAY:** Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

68. **GOOGLE VOICE:** Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web

browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

69. **YOUTUBE:** Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

70. **INTEGRATION OF GOOGLE SERVICES:** Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the

user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

71. **SUBSCRIBER RECORDS:** When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

72. **ACCESS RECORDS:** Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

73. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a

communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

74. **BROWSING, SEARCH, and APPLICATION USE HISTORY:** Google collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

75. **LOCATION HISTORY:** Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to

Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

76. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

77. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored

communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

78. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

79. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

80. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity,

documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

81. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users, their location(s) and activities at certain times relevant to the offenses at issue, the identities of their accomplices and co-conspirators, communications with those accomplices and co-conspirators, and actions taken and research performed relating to the criminal offenses at issue.

CONCLUSION

82. Based on the forgoing, I request that the Court issue the proposed search warrant.

83. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google LLC. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with khepp1020@gmail.com and kbehling916@gmail.com (the “accounts”) that are stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (“Google”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 17, 2022 with the Google Reference Number 25457714, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from April 19, 2021 to present, unless otherwise indicated:

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the accounts, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;
- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;
- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;
- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App Activity, including:

search terms; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
- **WEB-BASED CHATS:** The contents of all chats associated with the accounts, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;
- **MOBILE MESSAGING:** The contents of all messages associated with the accounts, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery numbers; usernames and other identifiers; user settings; and all associated logs and change history;

Google is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 666, 1343, and 371 and, since April 19, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters, persons, or entities:

- a. Records and information relating to the City of Milwaukee's property;
- b. Records and information relating to a conspiracy to defraud the City of Milwaukee;
- c. Records and information relating to communications with other City of Milwaukee employees, to include Lonnie Fischer, Kyle Hepp, and Kelly Behling;
- d. Records and information relating to communications with Richard Gillis, Linda Simcakoski, and other purchasers or potential purchasers of City of Milwaukee property;
- e. Records and information relating to the sale or resale of vehicles and equipment;
- f. Records and information relating to the origins or whereabouts of vehicles and equipment offered for sale;
- g. Records and information relating to the finances—including but not limited to expenditures, obligations, income, and any financial or monetary transfers—of Kyle Hepp, Kelly Behling, Lonnie Fischer, Richard Gillis, and Linda Simcakoski;
- h. Records and information relating to the deletion of electronic evidence;
- i. Records and information related to possible criminal prosecutions, relevant criminal laws, and investigative methods;
- j. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);

- k. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- l. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- m. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation, including interests and motivations; and
- n. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.